What is claimed is:

1. An anonymous fingerprinting method using a bilinear Diffie-Hellman problem, in a fingerprints embedment system that includes three participants, comprising the steps of:

(a) introducing system parameters shared by a first and a second participant, storing the system parameters in a memory of each of the first and the second participant and generating a public key and a secret key of the first participant;

(b) registering information on the first participant to a third participant based on the system parameters and the public and the secret key of the first participant, wherein the third participant issues a certificate based on the information on the first participant;

(c) at the second participant, authenticating a fairness of the first participant based on the certificate;

(d) embedding fingerprints into a digital content to be bought by the first participant; and

(e) when an illegal duplicate of the digital content or an illegally redistributed duplicate is found, identifying a traitor, who illegally duplicates the digital content or redistributes the illegally duplicated digital content, with the first participant based on the fingerprints embedded in the digital content.

2. The method of claim 1, wherein the step (a) includes the steps of:

(a1) generating G_1 and G_2, wherein G_1 is an elliptic curve group and G_2 is a cyclic multiplicative group;

(a2) taking a generator P out of the cyclic multiplicative group G_2;

(a3) calculating a bilinear map e on the groups G1 and G2 as follows:

$$e: G_1 \times G_1 \rightarrow G_2$$

(a4) storing the system parameters in a storage medium of the third participant and opening the system parameters so that the first and the second participant can use them, wherein the system parameters has G_1, G_2 and P;

(a5) selecting a secret key of the first participant out of G_2, wherein the secret key of the first participant is formed of s_1, s_2 and s_3; and

(a6) calculating a public key y_B of the first participant as follows:

$$y_B = e(P, P)^{s_1 s_2 s_3}.$$

3. The method of claim 2, wherein the step (b) includes the steps of:

(b1) generating a random value x_R corresponding to G2;

(b2) calculating a confidential value T_R as follows:

$$T_R = x_R P$$

and sending the confidential value T_R to the first

participant;

(b3) calculating pseudonym keys X and Y of the first participant as follows:

$$X = s_1 s_2 P$$

$$Y = s_1 s_2 s_3 P + T_R;$$

(b4) verifying validity of X and Y as follows:

$$e(Y, P) = y_B \cdot e(P, T_R);$$

(b5) calculating T as follows:

$$T = e(X, T_R)$$

and storing T in a memory of the third participant, wherein T is an intermediate value for judging whether or not the first participant is an owner of a secret key corresponding to the pseudonym keys X and Y;

(b6) issuing the certificate, which proves a fairness of the first participant to the second participant, and delivering the certificate to the first participant; and

(b7) at the first participant, calculating T' as follows:

$$T' = e(X, T_R)$$

and viewing (Y, T') as a pseudonym pair to safely store the pseudonym pair in a memory of the first participant, wherein T' is a value for notifying that the first participant is an owner of the secret key corresponding to X and Y.

4. The method of claim 3, wherein the step (c) includes the steps of:

(c1) sending the pseudonym pair and text to the second participant, wherein the text represents normal information about a digital content to be fingerprinted;

(c2) selecting a random value k out of G_2 to generate a B-DH signature Sig for the text, as follows:

$$Sig = sign(text, s_1, s_2, s_3, x_R, k);$$ and

(c3) verifying validity of the certificate and storing T' and the certificate as a purchase record of the first participant in a memory of the second participant.

5. The method of claim 4, wherein the step (d) includes the steps of:

(d1) at the first participant, sending x_R, Sig, s_1, s_2 and the certificate to the second participant and, at the second participant, presenting T', Y, em and the text to the first participant, wherein em denotes the digital content to be fingerprinted;

(d2) generating a specific value val_1 as follows:

$$val_1 = Verify_1 (text, sig, Y)$$

wherein val_1 is a Boolean variable to be seen by the second participant when verification of Sig is completed;

(d3) generating a particular value val_2 as follows:

$$val_2 = Verify_2(Y, Cert(Y|x_R), s_1, s_2, x_R, T)$$

wherein val_2 is a Boolean variable to be seen by the second participant when the certificate and Sig are respectively verified;

(d4) generating emb as follows:

$$emb = text \mid Sig \mid Y \mid Cert(Y|x_R) \mid s_1 \mid s_2 \mid x_R \mid T'$$

and storing emb in a memory of the second participant, wherein emb represents fingerprints to be embedded into the digital content em; and

(d5) obtaining a fingerprinted digital content em* as follows:

$$em^* = Fing(em, emb).$$

6. The method of claim 5, wherein the step (e) includes the steps of:

(e1) verifying validity of Sig for the text as follows:

$$T'' = e(s_1 s_2 P, x_R P)$$

wherein T" is a value for checking whether the first participant is an owner of a secret key corresponding to the pseudonym key Y'; and

(e2) determining an owner of the pseudonym key Y' to be the traitor if the pseudonym key Y' is given as follows:

$$e(Y', P) = y_B \cdot e(P, P)^{x_R}.$$

7. An anonymous fingerprinting apparatus using a bilinear Diffie-Hellman problem, comprising:

a registration authority;

a buyer; and

a merchant,

wherein the apparatus performs the steps of:

introducing system parameters shared by a first and a second participant, storing the system parameters in a memory of each of the first and the second participant and generating a public key and a secret key of each of the first and the second participant;

registering information on the first participant to a third participant based on the system parameters and the public and the secret key of the first participant, wherein the third participant issues a certificate based on the information of the first participant;

at the second participant, authenticating a fairness of the first participant based on the certificate;

embedding fingerprints into a digital content to be bought by the first participant; and

when an illegal duplicate of the digital content or an illegally redistributed duplicate is found, identifying a traitor, who illegally duplicates the digital content or redistributes the illegally duplicated digital content, with the first participant.